UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO:	CONFIRMATION NO.
09/921,536	08/03/2001	John R. McGarvey	5577-236	6803

58505 7590 11/09/2007
STEVENS & SHOWALTER, L.L.P.
BOX IBM
7019 CORPORATE WAY
DAYTON, OH 45459-4238

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
11/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/921,536	MCGARVEY ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 9/4/2007.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 9/4/2007 have been fully considered but they are not persuasive.

Regarding applicants' argument that neither Bartolomeos nor Kaliski teach a common nonce associated with each of a plurality of servers from an entity other than the client or the servers, the examiner does not find the argument persuasive for the reasons presented below.

First, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the applicants argue each of Bartolomeos and Kaliski individually, but fail to address what the combination of the teachings of these references would have suggested to the ordinary person of skill and creativity in the art at the time of invention.

Regarding applicants' argument that Kaliski fails to teach a common nonce being obtained from an entity other than the plurality of servers or the client, the examiner does not find the argument persuasive. Kaliski has not been relied upon as solely teaching this limitation. Rather, Kaliski teaches that the client can sign a message which contains a nonce for each server, wherein each nonce is received from its respective server, then nonces are placed into a single message at the client, which is then signed by the client. This can be seen in Kaliski Paragraphs 0083-0085. It is the teachings of Bartolomeos which have been relied upon as teaching that a

single server (middle tier server) provides the request for authentication data to the client for a multiplicity of servers, as can be seen on Page 13 Lines 9-11 and Line 24 - Page 14 Line 6. These teachings would suggest to the ordinary person skilled in the art that when employing the teachings of Kaliski in the authentication system of Bartolomeos, the nonces would be collected at a single server, and then transmitted in a single authentication request to the client. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that Kaliski does not teach a common nonce, but rather teaches independent nonces, the examiner does not find the argument persuasive. Each server's nonce, in Kaliski, is equivalent to the "nonce contributions" of the instant application. That is, each server's nonce is collected into a single message, as shown in Paragraph 0085 of Kaliski, and this message is signed. It is the message that is equivalent to the common nonce of the instant application. Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument that in Kaliski the client generates separate different messages, each containing a different signed nonce, and each being sent only to its respective server, the examiner does not find the argument persuasive. The applicants appear to have misread and/or misinterpreted the teachings of Kaliski. Clearly, in paragraph 0085, Kaliski teaches that "the recovery client 220 can generate 650 proof data by digitally signing **a message** containing **the various nonces**"." Kaliski further goes on to teach that each server verifies that its corresponding nonce was included in the signed message. Clearly, this teaches a common nonce, the message containing the various nonces, being signed and sent to the plurality of servers. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that in Kaliski, if the individual nonces were each sent to a middle tier server, the essence of the invention would be usurped, the examiner does not find the argument persuasive. This mere allegation is unsupported by any evidence. Nowhere does Kaliski teach that the nonces must be transmitted directly from the client to the server, and one of ordinary skill in the art would not come away with this conclusion upon reading Kaliski. Furthermore, the portion of Kaliski (the security of the strong secret data K) which the applicants argue would be ruined by collection of the nonces at a middle tier server, would not be jeopardized by collecting nonces at a middle tier server because the nonces are used for authenticating the client to the server, not for gaining access to the secret data.

Even further still, Bartolomeos is not concerned with the storage and protection of strong secret data K, but rather is concerned with authenticating the user of a client machine. Kaliski teaches a method of doing so using server nonces which are combined into a single message which is signed using the users private key, of a public/private key pair. In modifying the authentication system of Bartolomeos by the teachings of Kaliski, one of ordinary skill in the art would not find reason to include the teachings of Kaliski which regard the strong secret data, as this is not part of the authentication teachings of Kaliski. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that "each nonce" of Kaliski does not authenticate the client to the plurality of servers, the examiner does not find the argument persuasive. Again, the applicants have mischaracterized the reference and the rejection. The examiner points out that in the rejection, each nonce as taught by Kaliski is equivalent to a pre-nonce contribution of the instant invention, while the message containing the nonces as taught by Kaliski is equivalent to

the common nonce of the instant invention. It is the message containing the nonces which is signed by the client in order to provide authentication of the user to each of the servers. As such, the examiner does not find the argument persuasive.

Because the examiner has not found the arguments persuasive, the examiner has maintained the previously presented prior art rejections.

All objections and rejections not set forth below have been withdrawn.

Claims 1-32 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5, 7-11, 14-15, and 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartolomeos et al. (WO 99/56194) hereinafter referred to as Bartolomeos, and further in view of Kaliski, JR. (Patent Application Publication 2001/0055388) hereinafter referred to as Kaliski.

Regarding claim 1, Bartolomeos disclosed a method for a middle-tier server (See Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element 110(I)) to a plurality of servers (See Bartolomeos Servers 120(2)-120(M)), the method comprising:

providing a request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11); receiving the authentication data at the middle-tier server (See Bartolomeos Page 13 Lines 9-11); and providing authentication data to the plurality of servers to authenticate the client to the plurality of servers (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers, and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been

obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 26, Bartolomeos disclosed a system for a middle-tier server (See Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element 110(I)) to a plurality of servers (See Bartolomeos Servers 120(2)-120(M)), comprising: means for providing a request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11); means for receiving the authentication data at the middle-tier server (See Bartolomeos Page 13 Lines 9-11); and means for providing authentication data to the plurality of servers to authenticate the client to the plurality of servers (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate

the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers, and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client.

This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 27, Bartolomeos a computer program product for a middle-tier server (See Bartolomeos Fig. 1 Server 120(I)) to impersonate a client (See Bartolomeos Element 110(I)) to a plurality of servers (See Bartolomeos Servers 120(2)-120(M)), comprising: a computer readable media having computer readable program code embodied therein, the computer readable program code comprising: computer readable program code that provides a request for authentication data to the client (See Bartolomeos Page 13 Lines 9-11); computer readable program code that receives the authentication data at the middle-tier server (See Bartolomeos Page 13 Lines 9-11); and computer program readable code that provides authentication data to the plurality of servers to authenticate the client to the plurality of servers (See Bartolomeos Page 13 Line 24 – Page 14 Line 6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines

6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers, and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating

repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 28, Bartolomeos disclosed a method of authenticating a client (See Bartolomeos Fig. 1 Element 100(I)), comprising: receiving at a server (See Bartolomeos Fig. 1 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements 120(2)-120(M)), authentication data that is provided to each of the plurality of servers (See Bartolomeos Page 14 Lines 1-4) from an entity other than the client or the plurality of servers (See Bartolomeos Page 14 Lines 1-4 server 120(1)), the authentication data being associated with each of the plurality of servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11); and authenticating the client based on the received authentication data (See Bartolomeos Page 14 Lines 5-6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers,

and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the

nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 31, Bartolomeos disclosed a system for authenticating a client (See Bartolomeos Fig. 1 Element 100(I)), comprising: means for receiving at a server (See Bartolomeos Fig. 1 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements 120(2)-120(M)), authentication data that is provided to each of the plurality of servers (See Bartolomeos Page 14 Lines 1-4) from an entity other than the client or the plurality of servers (See Bartolomeos Page 14 Lines 1-4 server 120(1)), the authentication data being associated with each of the plurality of servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11); and means for authenticating the client based on the received authentication data (See Bartolomeos Page 14 Lines 5-6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers, and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the

signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 32, Bartolomeos disclosed a computer program product for authenticating a client (See Bartolomeos Fig. 1 Element 100(I)), comprising: a computer readable media having computer program code embodied therein, the computer readable program code comprising: computer readable program code which receives at a server (See Bartolomeos Fig. 1 Element 120(2)) of a plurality of servers (See Bartolomeos Fig. 1 Elements 120(2)-120(M)), authentication data that is provided to each of the plurality of servers (See Bartolomeos Page 14 Lines 1-4) from an entity other than the client or the plurality of servers (See Bartolomeos Page 14 Lines 1-4 server 120(1)), the authentication data being associated with each of the plurality of servers (See Bartolomeos Page 14 Lines 5-6 and Page 11 Lines 6-11); and computer readable program code which authenticates the client based on the received authentication data (See Bartolomeos Page 14 Lines 5-6), but Bartolomeos failed to disclose that the authentication data was a common nonce associated with the plurality of servers, or that the common nonce was signed by the client prior to being used to authenticate the client. However, Bartolomeos did suggest that any type of authentication could have been used, and that the disclosed username and password were simply one embodiment (See Bartolomeos Page 11 Lines 6-11), and Bartolomeos did disclose only server 120(1) contacting the client to request the client's authentication data (See Bartolomeos Page 13 Lines 9-11).

Kaliski teaches a method for a client to authenticate itself to multiple servers by signing a message with the clients private key, the message containing a nonce from each of the servers, and the private key being of a public/private key pair. Kaliski further teaches that the signed message is returned to server, wherein the client is authenticated if the server verifies the

signature of the message, as well as verifying that the message contains its corresponding nonce (See Kaliski Paragraph 0069 and 0083-0086, particularly 0085).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kaliski in the client authentication system of Bartolomeos by having each server provide a nonce for the client, having the client sign a message containing the nonces, having the client return the signed message to server 120(1), authenticating the client using the message, and if authenticated, providing the signed message to each of servers 120(2)-120(M) which then use the signed message to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more secure authentication than User ID and Password, and further would have been motivated to ensure that the authentication data is fresh and not a replay of previous authentication data.

In this combination, it further would have been obvious to the ordinary person skilled in the art at the time of invention for Server 120(1) to have collected the nonces from Servers 120(2)-120(M) and provided them to the client in a single message as a challenge to the client. This would have been obvious because Bartolomeos disclosed only server 120(1) requesting authentication data from the client, and furthermore Bartolomeos is concerned with eliminating repetitive, tedious and burdensome tasks, and one of ordinary skill in the art would have recognized that sending an individual nonce message for each of the M servers would have been repetitive, tedious, and burdensome. Furthermore, sending one message containing all the nonces to the client would have been obvious because the ordinary person skilled in the art would have been motivated to eliminate unnecessary traffic through network 110.

Regarding claim 2, the combination of Bartolomeos and Kaliski disclosed that the step of obtaining a common nonce comprises the step of generating, by an entity other than the client (110(1)) or the plurality of servers (120(2)-120(M)), a common nonce based on information obtained from each of the plurality of servers (See Kaliski Paragraphs 0083-0086 as well as the rejection of claim 1 above, wherein server 120(1) generates the message).

Regarding claim 3, the combination of Bartolomeos and Kaliski disclosed that the step of generating a common nonce comprises the steps of: obtaining pre-nonce contributions from the plurality of servers (See Kaliski Paragraphs 0083-0086); combining the pre-nonce contributions to provide a single pre-nonce token (See Kaliski Paragraph 0085 and the rejection of claim 1 above); and providing the common nonce based on the pre-nonce token (See the rejection of claim 1 above).

Regarding claim 5, the combination of Bartolomeos and Kaliski disclosed that the step of combining the pre-nonce contributions to provide a single pre-nonce token comprises concatenating the pre-nonce contributions (See Kaliski Paragraph 0085 and the rejection of claim 1 above).

Regarding claim 7, the combination of Bartolomeos and Kaliski disclosed that the step of obtaining pre-nonce contributions comprises the steps of requesting a pre-nonce contribution from each of the plurality of servers and receiving the pre-nonce contributions from the plurality of servers (See Kaliski Paragraph 0083 and the rejection of claim 1 above).

Regarding claims 8-10, the combination of Bartolomeos and Kaliski disclosed that requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of servers (See Kaliski paragraph 0083 and the rejection of claim 1 above); wherein the

authenticated requests are encrypted, and include a source of the request (wherein it was well known in the art of information security at the time of invention to use authenticated requests, to encrypt communications, and to include the source of a message with the message).

Regarding claim 11, the combination of Bartolomeos and Kaliski disclosed that the pre-nonce contributions include at least one of an identification of a server of the plurality of servers and a random number (See Kaliski Paragraphs 0083-0086).

Regarding claim 14, the combination of Bartolomeos and Kaliski disclosed receiving a transaction identification from a trusted server of the plurality of servers and associating the transaction identification with the common nonce (See Kaliski Paragraph 0085 and the rejection of claim 1 above).

Regarding claim 15, the combination of Bartolomeos and Kaliski disclosed tracking use of the common nonce based on the transaction identification (See Kaliski Paragraph 0085 and the rejection of claim 1 above).

Regarding claim 29, the combination of Bartolomeos and Kaliski disclosed that the common nonce is provided by a trusted third party (See the rejection of claim 28 above, wherein the common nonce is provided by the server 120(1)).

Regarding claim 30, the combination of Bartolomeos and Kaliski disclosed that the common nonce is generated by an entity other than the client or the plurality of servers based on information provided by each of the plurality of servers (See the rejection of claim 28 above).

Claims 4, 6, 12-13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Bartolomeos and Kaliski as applied to claim 3 above, and further in view of Schneier (Applied Cryptography).

Regarding claim 4, the combination of Bartolomeos and Kaliski disclosed providing a common nonce (See Kaliski Paragraph 0085 and the rejection of claim 1 above), but failed to disclose reducing the nonce challenges to provide the common nonce. However, the combination of Bartolomeos and Kaliski did disclose digitally signing a message containing the nonce challenges (See the rejection of claim 1 above).

Schneier teaches that when digitally signing a message, it is practical to hash the message and encrypt the hash, with a private key, as the signature, rather than encrypting the whole message (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions). Schneier also teaches that in such a system, to verify the signature, the verifier hashes the message, decrypts the signed hash with the signers public key, and verifies that the two hashes are the same (See Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the digital signatures of the combination of Bartolomeos and Kaliski by providing a hash of the nonce message instead of the whole nonce message for signing. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the speed of the signing method, as well as reduce the amount of data needing to be transmitted to the client.

Regarding claim 6, the combination of Bartolomeos, Kaliski, and Schneier disclosed that the step of reducing the pre-nonce token to provide the common nonce comprises the step of hashing the pre-nonce token utilizing a one-way hash function so as to provide the common nonce (See the rejection of claim 4 above).

Regarding claim 20, the combination of Bartolomeos, Kaliski, and Schneier disclosed that at least one of the plurality of servers carries out the steps of: receiving the signed common nonce, the common nonce and the pre-nonce token; hashing the received pre-nonce token; comparing the hashed pre-nonce token to the common nonce; indicating that the client is not authenticated if the hashed pre-nonce token is different from the common nonce (See Kaliski Paragraph 0085 and Schneier Page 38 Section Signing Documents with Public-Key Cryptography and One-Way Hash Functions).

Regarding claims 12-13, the combination of Bartolomeos and Kaliski disclosed the client checking the nonce challenge from the server for requisite strength, and aborting the authentication process if the nonce challenge did not meet the requisite strength (See Kaliski Paragraph 0084), but failed to disclose that this check included checking the signature of the nonce challenge to verify that it was signed by the server.

Schneier teaches that digital signatures provide a means for verifying the sender of a message (See Schneier Page 37 Signing Documents with Public Key Cryptography).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the nonce challenge system of Bartolomeos and Kaliski by having the servers 120(2)-120(M) sign the challenges and having the server 120(1) verify the signature of the challenges before using the challenges. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against illicit alteration of the challenge nonce.

Claims 16-19, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Bartolomeos and Kaliski as applied to claim 3 above, and further in view of Menezes et al. (Handbook of Applied Cryptography).

Regarding claim 21, the combination of Bartolomeos and Kaliski disclosed the server receiving the nonce challenges, and authenticating the client based on whether the nonce challenges included the nonce challenge of the server (See Kaliski Paragraph 0085), but failed to disclose that the nonce challenges included random numbers.

Menezes teaches that nonce challenges can be random numbers (See Menezes Page 398).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the nonce challenge system of the combination of Bartolomeos and Kaliski by having the nonce challenges be random numbers. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide uniqueness and timeliness assurances in the system in order to avoid replay and interleaving attacks.

Regarding claims 16-17, and 22 the combination of Bartolomeos and Kaliski disclosed a plurality of servers providing nonce challenges to a client in order to authenticate the client, and verifying the nonce in the response to the challenge (See Kaliski Paragraphs 0083-0085) but failed to disclose giving the nonce an expiration time and further authenticating the client based on the expiration time.

Menezes teaches that when using nonce challenges the challenger should apply a timeout period to the nonce and not authenticate the client if the response is received after the timeout period has expired (See Menezes Page 398 Section (i).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the nonce challenge system of the combination of Bartolomeos and Kaliski by applying and checking a timeout period to the nonce when authenticating a client. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against replay and interleaving attacks.

Regarding claims 18-19, the combination of Bartolomeos and Kaliski disclosed using a users public key to verify the signature of the nonce message by verifying that the signature corresponded to the signature of the clients private/public key pair (See Kaliski Paragraph 0085), but failed to disclose that the verifying server got the public key from a public key certificate and also failed to disclose that the authentication would fail if the certificate was not trusted.

Menezes teaches that public key certificates are a means to store, distribute, and forward public keys without danger of undetectable manipulation. Menezes also teaches that when using a certificate for authentication, the certificate is received, the expiration date is checked, the certification authority validity is checked, the signature of the certificate is checked, and the certificate is checked to see if it has been revoked, and if these checks pass then the public key is valid (See Menezes Pages 559-560).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the authentication system of the combination of Bartolomeos and Kaliski by obtaining the public key from a public key certificate and verifying that the certificate is valid in order to use the public key to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against undetected manipulation of the public key.

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Bartolomeos and Kaliski as applied to claim 1 above, and further in view of Day (US Patent Number 6,052,784).

The combination of Bartolomeos and Kaliski disclosed a challenge nonce system (See Kaliski Paragraphs 0083-0086) but failed to disclose the nonce being received from a trusted third party and verifying the signature of the trusted third party.

Day teaches that a nonce can be signed by a trusted third party in order to authenticate the nonce (See Day Col. 3 Paragraph 5).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Day in the nonce challenge system of the combination of Bartolomeos and Kaliski by having the nonce challenges signed by a certification authority prior to sending the challenge to the client, and verifying the signature on the nonce. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent the nonce from being illicitly undetectably modified prior to the client receiving the nonce challenge.

Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Bartolomeos, Kaliski, and Day as applied to claim 23 above, and further in view of Menezes.

The combination of Bartolomeos, Kaliski, and Day disclosed using a users public key to verify the signature of the nonce message by verifying that the signature corresponded to the signature of the clients private/public key pair (See Kaliski Paragraph 0085), but failed to

disclose that the verifying server got the public key from a public key certificate and also failed to disclose that the authentication would fail if the certificate was not trusted.

Menezes teaches that public key certificates are a means to store, distribute, and forward public keys without danger of undetectable manipulation. Menezes also teaches that when using a certificate for authentication, the certificate is received, the expiration date is checked, the certification authority validity is checked, the signature of the certificate is checked, and the certificate is checked to see if it has been revoked, and if these checks pass then the public key is valid (See Menezes Pages 559-560).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the authentication system of the combination of Bartolomeos, Kaliski, and Day by obtaining the public key from a public key certificate and verifying that the certificate is valid in order to use the public key to authenticate the client. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against undetected manipulation of the public key.

Conclusion

Claims 1-32 have been rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew Henning/
Assistant Examiner
Art Unit 2131
11/6/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100